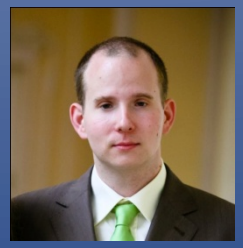
An Efficient and Robust Social Network De-anonymization Attack

Joint work with B. Simon, S. Imre

WPES'16, 2016-10-24

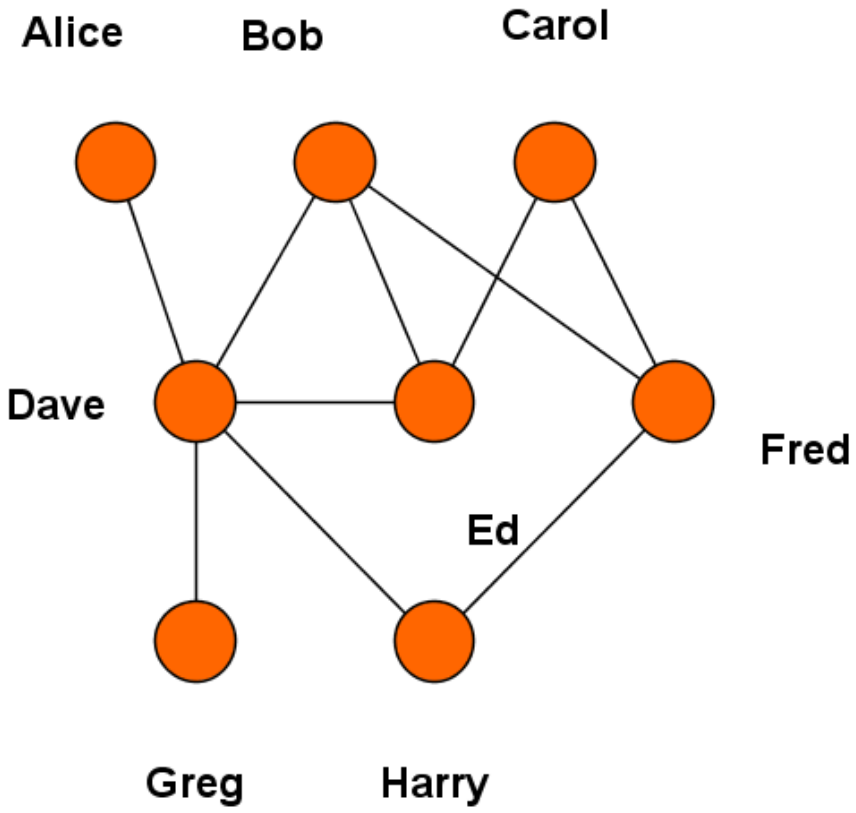
Gábor György Gulyás
Postdoc @ Privatics
http://gulyas.info // @GulyasGG



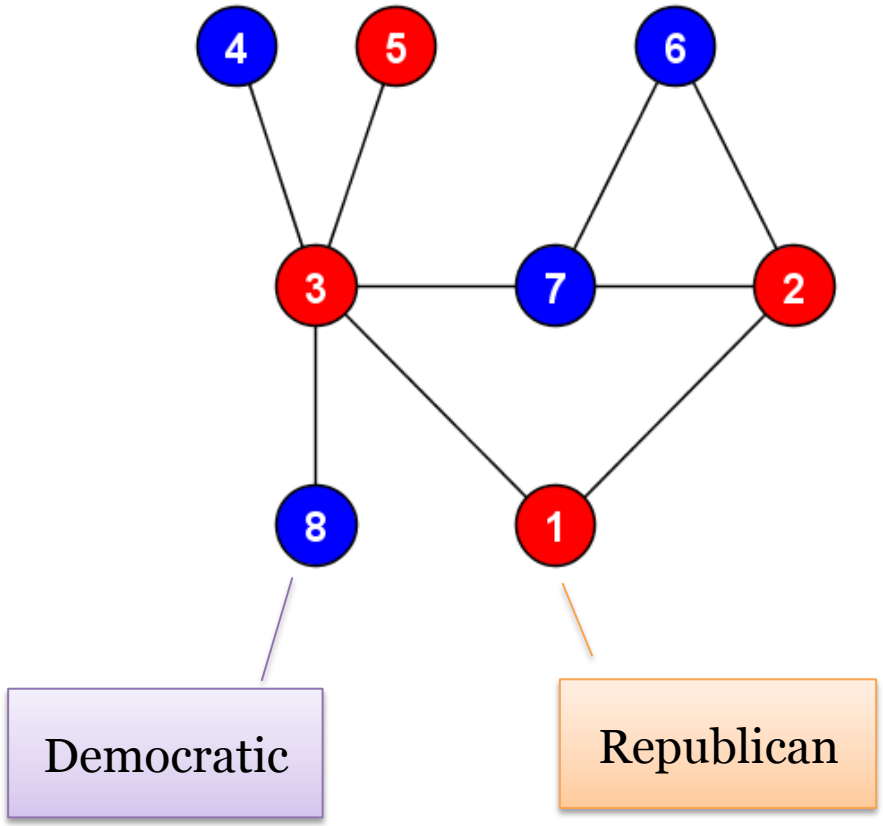
INVENTEURS DU MONDE NUMÉRIQUE

Re-identification using the structure

Auxiliary information, G_{src}
(a public crawl, e.g., Flickr)



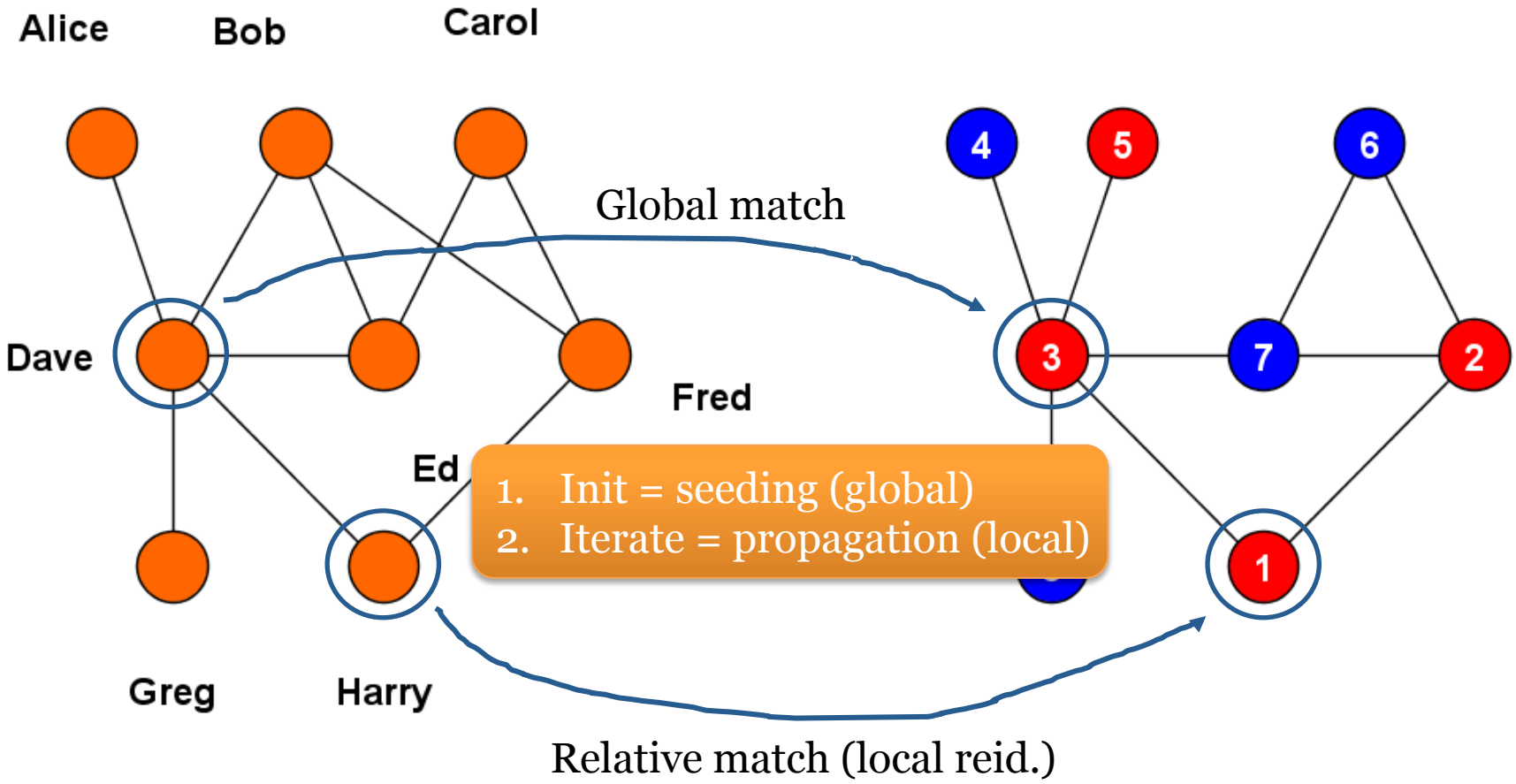
Anonimized graph, G_{tar}
(anonimized export, e.g., Twitter)



Re-identification using the structure (2)

Auxiliary information, G_{src}
(a public crawl, e.g., Flickr)

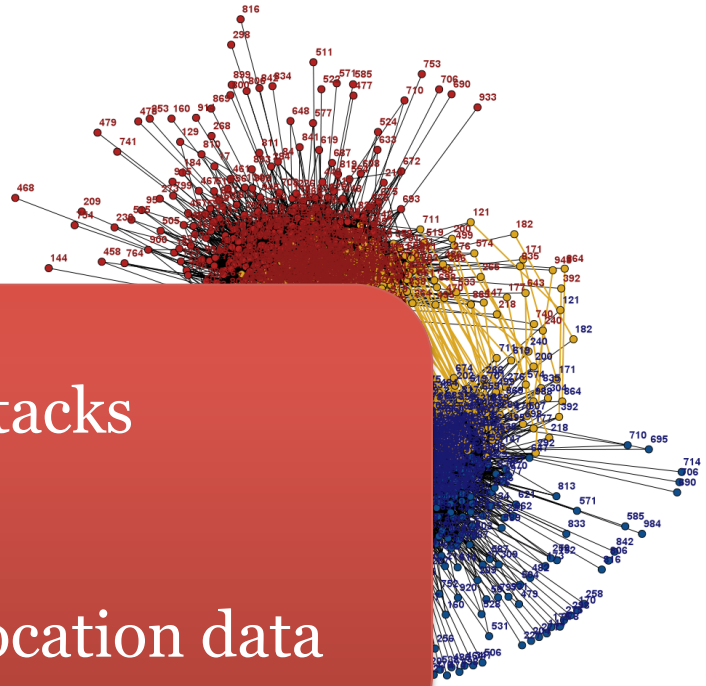
Anonimized graph, G_{tar}
(anonimized export, e.g., Twitter)



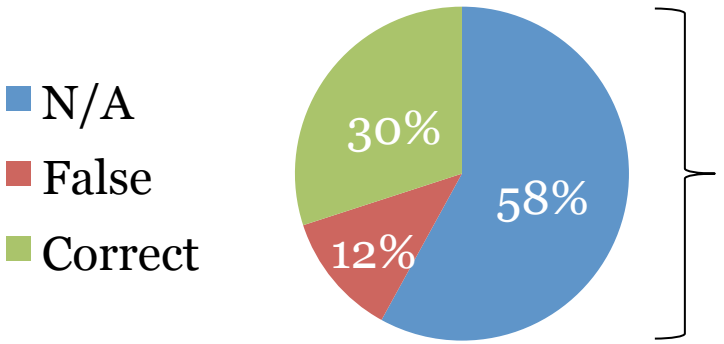
Narayanan&Shmatikov results (Nar09)

- Large social networks
  - Background knowledge: Flickr (3,3
  - An
    Tw
    (22

%

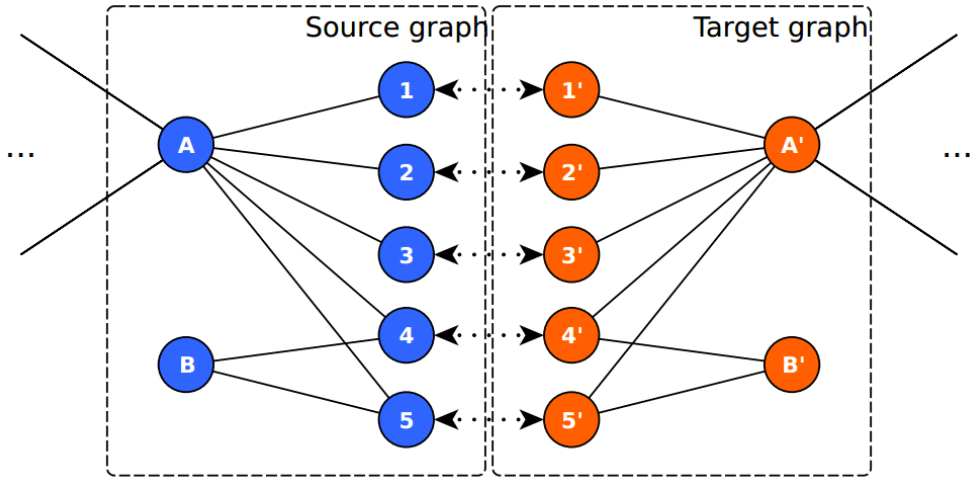


- De-anonymization attacks
- Linking attacks
- Re-identification of location data



Ground truth of 27k nodes
(verified by name/user/loc.)

Motivation for Bumblebee



$$\mathrm{NarSim}(v_i, v_j) = \frac{\#\mathrm{mutual\_nbrs}}{\sqrt{\deg(v_j)}}$$

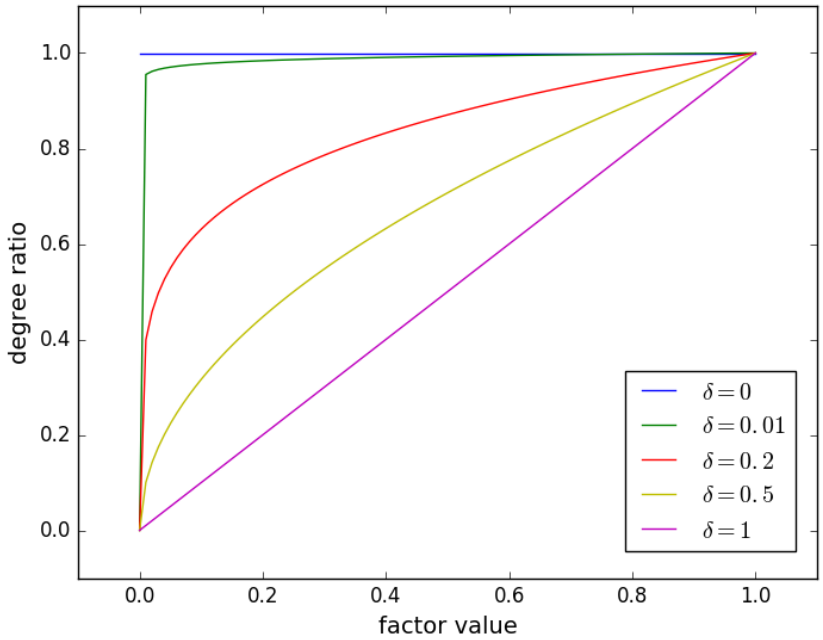
$$\mathrm{BlbSim}(v_i, v_j) = \#\mathrm{mutual\_nbrs} \cdot \left(\min\left(\frac{\deg(v_i)}{\deg(v_j)}, \frac{\deg(v_j)}{\deg(v_i)} \right) \right)^{\delta}$$

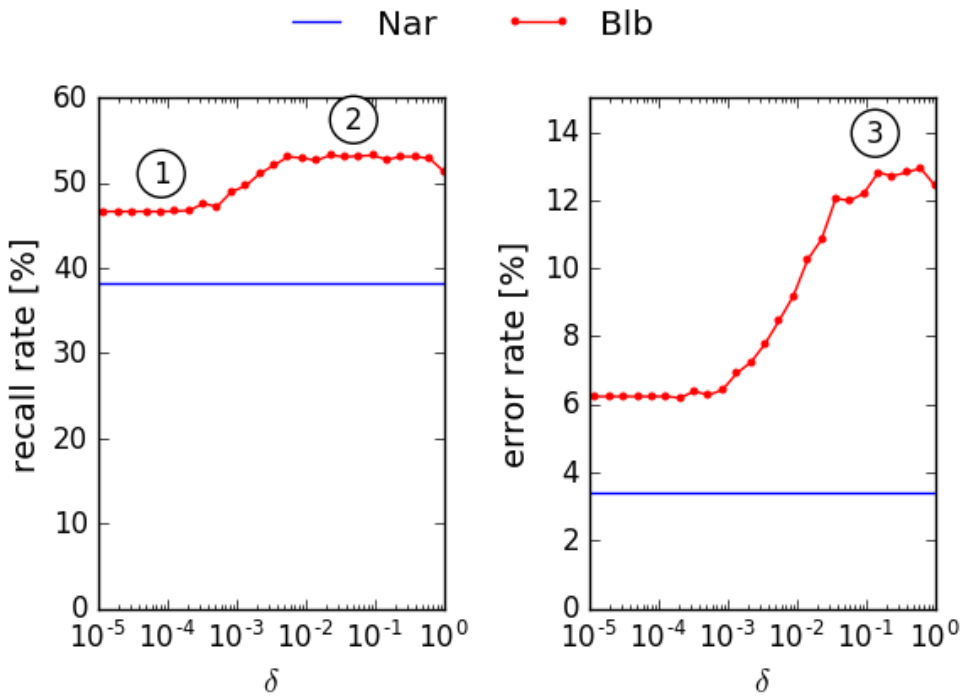
	A'	B'	?
A	$\frac{5}{\sqrt{100}}$	$\frac{2}{\sqrt{2}}$	B'
B	$\frac{2}{\sqrt{100}}$	$\frac{2}{\sqrt{2}}$	B'

	A'	B'	?
A	5	0.89	A'
B	0.89	2	B'

Parameters of the attack – δ

$$\mathrm{BlbSim}(v_i, v_j) = \#\mathrm{mutual\_nbrs} \cdot \left(\min\left(\frac{\deg(v_i)}{\deg(v_j)}, \frac{\deg(v_j)}{\deg(v_i)} \right) \right)^{\delta}$$





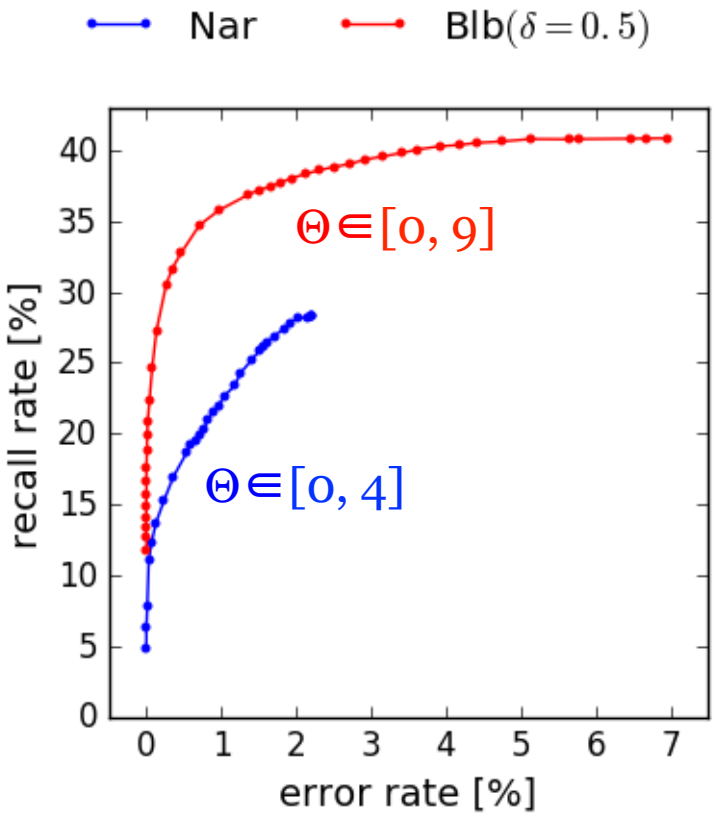
Visual playground: https://gulyas.info/snda

Parameters of the attack (2) – Θ

Algorithm 1: PROPAGATE

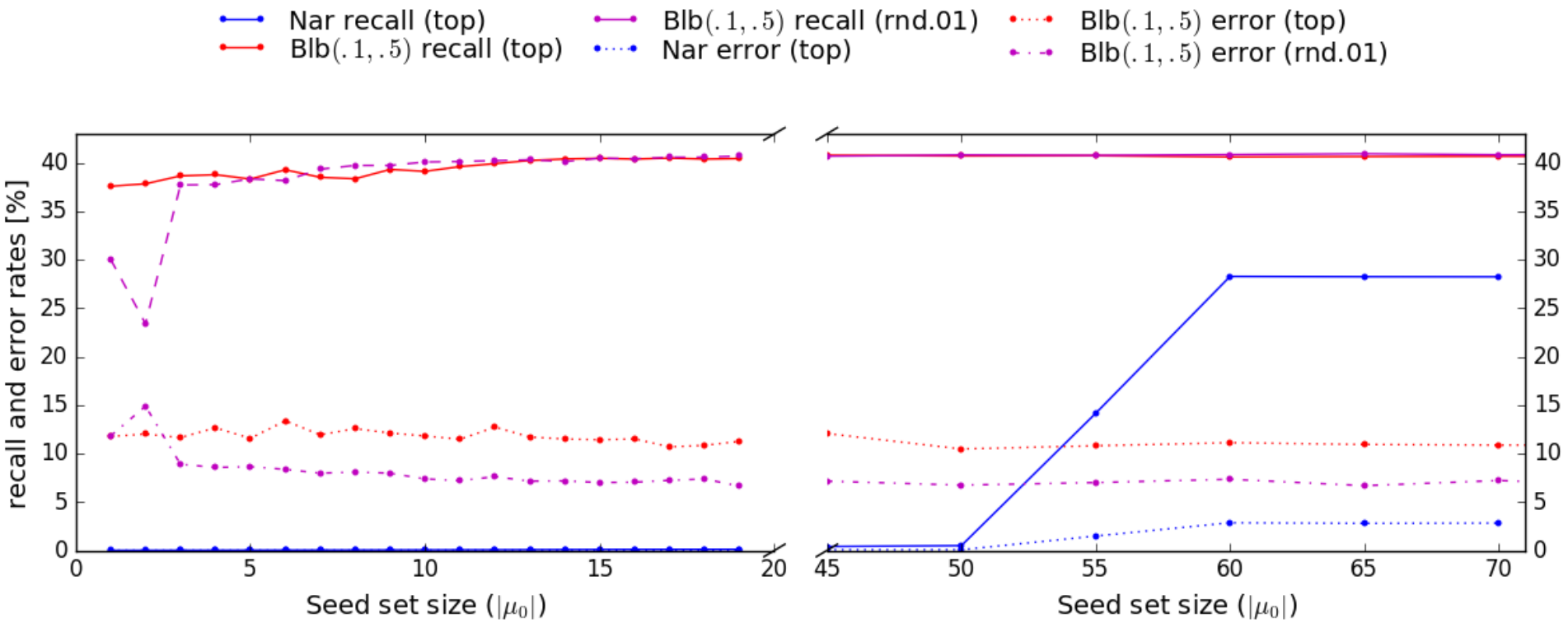
Data: G_{src}, G_{tar}, μ
Result: μ, Δ

$\Delta \leftarrow 0$;
for $v_{src} \in V_{src}$ **do**
  $S \leftarrow \text{SCORE}(G_{src}, G_{tar}, v_{src}, \mu)$;
  if $\text{ECC}(S.\text{VALUES}()) < \Theta$ **then**
    CONTINUE;
  end
  $v_c \leftarrow \text{RANDOM}(\text{MAX}(S))$;
  $S_r \leftarrow \text{SCORE}(G_{tar}, G_{src}, v_c, \mu^{-1})$;
  if $\text{ECC}(S_r.\text{VALUES}()) < \Theta$ **then**
    CONTINUE;
  end
  $v_{rc} \leftarrow \text{RANDOM}(\text{MAX}(S_r))$;
  if $v_{src} = v_{rc}$ **then**
    $\mu[v_{src}] \leftarrow v_c$;
    $\Delta \leftarrow \Delta + 1$;
  end
end



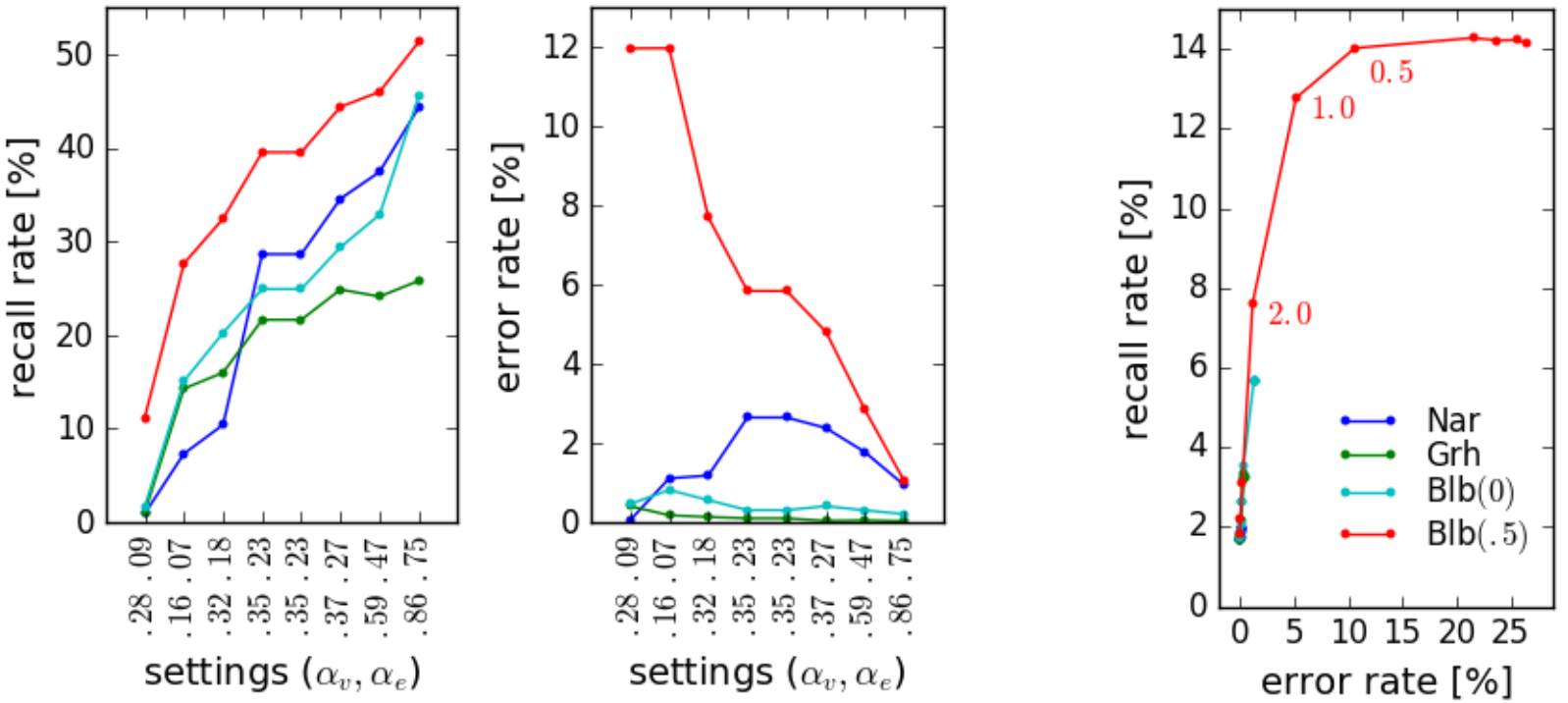
Visual playground: https://gulyas.info/snda

Seeding sensitvity



Visual playground: https://gulyas.info/snda

Robustness to noise



Visual playground: https://gulyas.info/snda

Comparison with other attacks

SecGraph: A Uniform and Open-source Evaluation System for Graph Data Anonymization and De-anonymization

Shouling Ji
Georgia Institute of Technology

Weiqing Li
Georgia Institute of Technology

Prateek Mittal
Princeton University

Xin Hu
IBM Thomas J. Watson Research Center

Raheem Beyah
Georgia Institute of Technology

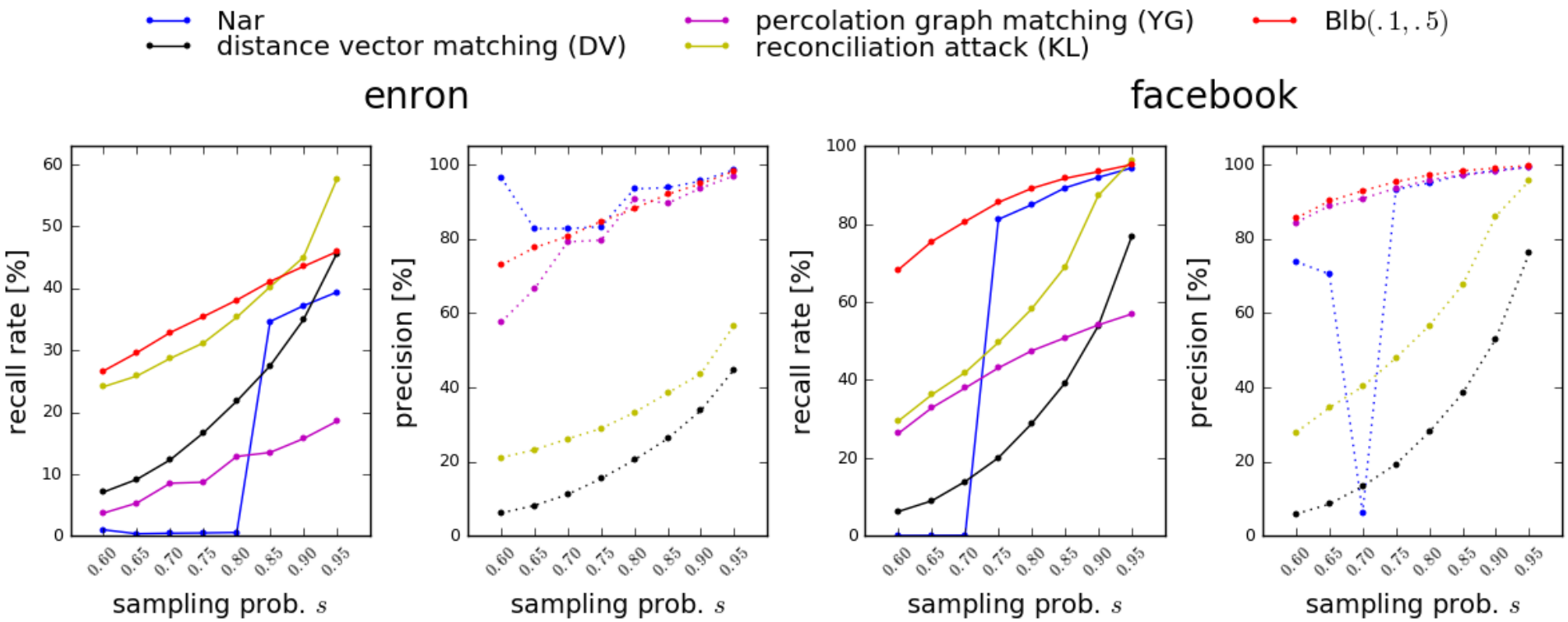
Abstract

In this paper, we analyze and systematize the state-of-the-art graph data privacy and utility techniques. Specifically, we propose and develop *SecGraph* (available at [1]), a uniform and open-source Secure Graph data sharing/publishing system. In SecGraph, we systematically study, implement, and evaluate 11 graph data anonymization algorithms, 19 data utility metrics, and 15 modern Structure-based De-Anonymization (SDA) attacks. To the best of our knowledge, SecGraph is the first such system that enables data owners to anonymize data by state-of-the-art anonymization techniques, measure the data's utility, and evaluate the data's vulnerability against modern De-Anonymization (DA) attacks. In

called *graph data*. For research purposes, data and network mining tasks, and commercial applications, these graph data are often transferred, shared, and/or provided to the public, research community, and/or commercial partners. Since graph data carry a lot of sensitive private information of users/systems who generated them [2, 3], it is critical to protect users' privacy during the data transferring, sharing, and/or publishing.

To protect users' privacy, several anonymization techniques have been proposed to anonymize graph data, which can be classified into six categorizes: Naive ID Removal, Edge Editing (EE) based techniques [6], *k*-anonymity based techniques [7–11], Aggregation/Class/Cluster based techniques [12–14], Differen-

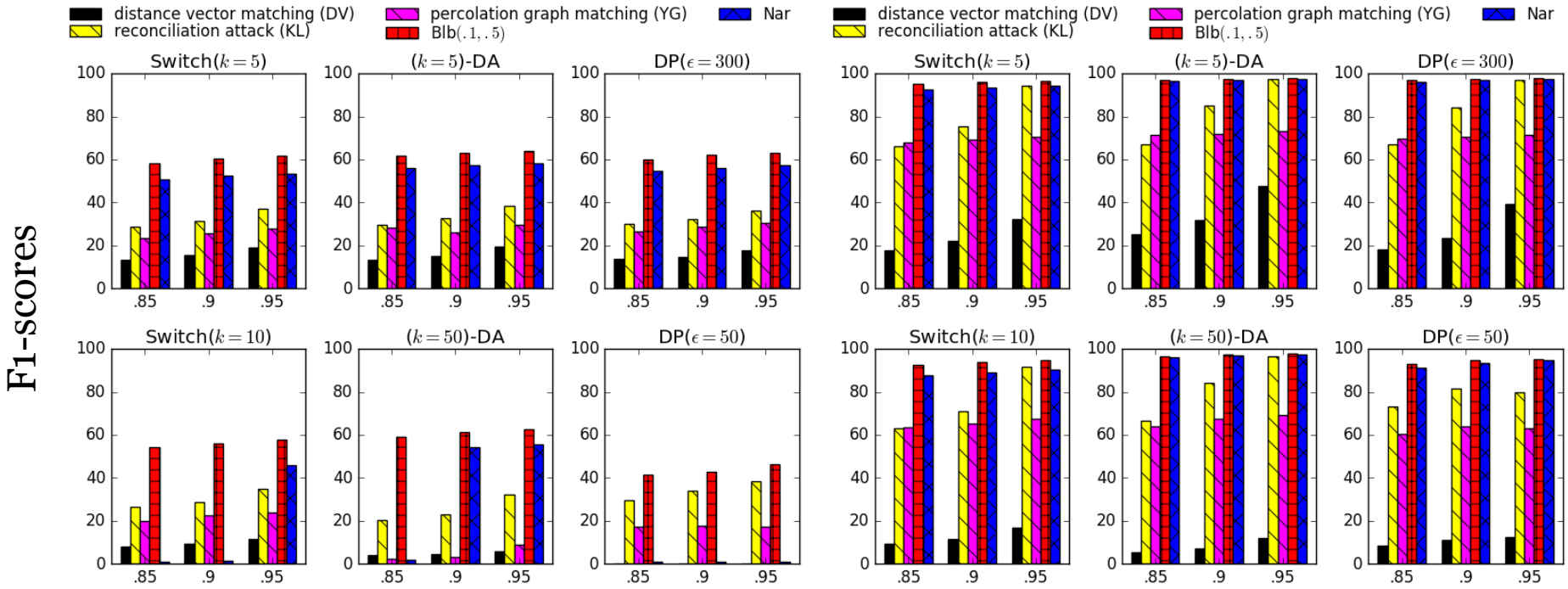
Comparison with other attacks (2)



Comparison with other attacks (3)

Enron (36k)

Facebook (63k)



$$\mathrm{F1} = 2 \cdot \frac{\mathrm{Precision} \cdot \mathrm{Recall}}{\mathrm{Precision} + \mathrm{Recall}}$$

Conclusion

- We proposed a new attack based on a new scoring scheme, and showed its superiority to all existing attacks.

- Visual playground & Python code:

  https://gulyas.info/snda

- Seriously interested? Try out SALab, our framework for social network de-anonymization:

  https://github.com/gaborgulyas/salab

Thank you for your attention!

ANY QUESTIONS?

Gábor György Gulyás
Postdoc @ Privatics
http://gulyas.info // @GulyasGG